REMARKS

In response to the Office Action, Claims 1, 20-22, 24 and 38-40 are amended. Claims 2, 6, 7, 27, and 28 were previously canceled. Claims 1, 3-5, 8-26 and 29-41 remain in the Application. Reconsideration of the pending claims is respectfully requested in view of the above amendments and the following remarks.

I. Claims Rejected Under 35 U.S.C. §103

A. Claims 1, 3-5, 8-22, 24-26 and 29-41 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,953,424 issued to Vogelesang et al. ("Vogelesang"), in view of Menezes, Alfred J., Handbook of Applied Cryptography, CRC Press, 1997, pages 234-237 ("Menezes") in view of *Simple Network Authenticating Key Exchange* ("SNAKE") and further in view of U.S. Patent No. 6,307,938 issued to Matyas, Jr. et al. ("Matyas").

To establish a *prima facie* case of obviousness, the relied upon references must teach or suggest every limitation of the claim such that the invention as a whole would have been obvious at the time the invention was made to one skilled in the art.

Independent Claims 1, 20-22, 24 and 38-40 include the following elements or analogous elements of:

> "generating, at the first entity, a first secret S_B by hashing one or more parameters that are known to the first entity and the second entity, at least one of the parameters being a result of hashing one or more of the following: a first password P_B, the first public key M_B, and the second public key M_A".

Applicants submit that the cited references, separately or in combination, do not teach or suggest these elements.

Vogelesang discloses a cryptographic system in which signals between two participants are encrypted with one encryption key. The Examiner recognizes that Vogelesang does not disclose encryption with two encryption keys, but relies on Menezes to disclose double encryption, and SNAKE to disclose the generation of the first secret S_B. The Examiner further relies on Matyas for disclosing the creation of a secret equal to a sequence of hash functions applied to different values.

Without conceding the Examiner's assertion, Applicants submit that none of the references disclose hashing one or more parameters with at least one of the parameters being the result of hashing other values. Matyas discloses the use of multiple hash functions, with each hash functions applied to a different seed to generate a different portion of a final value. These different portions are then concatenated to form the final value (col. 6, lines 4-20). Matyas does not disclose hashing the result of hashing one or more values. Vogelesang, Menezes and SNAKE also do not disclose this feature. Thus, the cited references cannot be properly interpreted as disclosing the elements as recited in independent Claims 1, 20-22, 24 and 38-40, as well as their respective dependent claims. Accordingly, reconsideration and withdrawal of the §103 rejection of Claims 1, 3-5, 8-22, 24-26 and 29-41 are respectfully requested.

B. Claim 23 stands rejected under 35 U.S.C. §103(a) as being unpatentable over the modified Vogelesang, Menezes, SNAKE and Matyas system.

Claim 23 depends from Claim 22 and incorporates the limitations thereof. Thus, for at least the reasons mentioned above in regard to Claim 22, the cited references do not teach or suggest each of the elements of Claim 23.

In the rejection of Claim 23, the Examiner recognizes that the modified Vogelesang, Menezes, SNAKE and Matyas system does not disclose that the first public key M_B is transmitted with the encrypted random nonce, but has taken an official notice that this feature would have been obvious to one of ordinary skill in the art at the time the invention was filed. However, Vogelesang discloses transmitting a public signal X before transmitting an encrypted random nonce (col. 16, lines 25-67). There is no indication in Vogelesang, Menezes, SNAKE or Matyas that a public key is transmitted with an encrypted random nonce. Thus, the official notice taken by the Examiner is not supported by any of the cited references and is purely based on hindsight construction.

Applicants further submit that the rejection of Claim 23 was traversed in the previous response based on its dependency from an amended independent claim. Therefore, Applicants have not acquiesced to the rejection of Claim 23. Accordingly, reconsideration and withdrawal of the §103 rejection of Claim 23 are requested.

CONCLUSION

In view of the foregoing, it is believed that all claims are now in condition for allowance and such action is earnestly solicited at the earliest possible date. If there are any additional fees due in connection with the filing of this response, please charge those fees to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: March 14, 2008

/Tong J. Lee/
Tong J. Lee, Reg. No. 48,582

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(310) 207-3800

CERTIFICATE OF ELECTRONIC FILING
I hereby certify that this correspondence is being submitted electronically via EFS Web on the date shown below

Marilyn Bass March 14, 2008